U.S. ENVIRONMENTAL PROTECTION AGENCY

OFFICE OF INSPECTOR GENERAL

Operating efficiently and effectively

EPA Needs to Improve Processes for Securing Region 8's Local Area Network

Report No. 20-E-0309

September 10, 2020

Report Contributors:

Rudolph M. Brevard
Nii-Lantei Lamptey
Christina Nelson
Teresa Richardson
Albert Schmidt

Abbreviations

CIO	Chief Information Officer
EPA	U.S. Environmental Protection Agency
LAN	Local Area Network
NCC	National Computer Center
OCFO	Office of the Chief Financial Officer
OIG	Office of Inspector General
OMS	Office of Mission Support
PII	Personally Identifiable Information
SCORPIOS	Superfund Cost Recovery Package Imaging and Online System

Cover Photo: The Office of Mission Support conducts vulnerability tests of local area networks at Region 8's headquarters, laboratory, and Montana office. (EPA OIG graphic)

Are you aware of fraud, waste, or abuse in an EPA program?

EPA Inspector General Hotline
1200 Pennsylvania Avenue, NW (2431T)
Washington, D.C. 20460
(888) 546-8740
(202) 566-2599 (fax)
OIG_Hotline@epa.gov

Learn more about our OIG Hotline.

EPA Office of Inspector General
1200 Pennsylvania Avenue, NW (2410T)
Washington, D.C. 20460
(202) 566-2391
www.epa.gov/oig

Subscribe to our Email Updates
Follow us on Twitter @EPAoig
Send us your Project Suggestions

U.S. Environmental Protection Agency
Office of Inspector General

20-E-0309
September 10, 2020

At a Glance

Why We Did This Project

The U.S. Environmental Protection Agency's Office of Inspector General performed this evaluation to (1) assess the completeness of the EPA's processes for testing its network to identify potential vulnerabilities that could compromise the Agency's systems and data, and (2) conduct an independent automated vulnerability testing of information technology resources connected to the EPA's network to identify vulnerabilities that could compromise the confidentiality, integrity, and availability of Agency information systems and data.

We performed our evaluation at EPA headquarters, Region 8, and the National Computer Center. Due to travel restrictions, we only performed OIG vulnerability testing at the Region 8 headquarters and laboratory and on the Region 8 Superfund Cost Recovery Package Imaging and Online System, known as SCORPIOS, server.

This report addresses the following:

- *Operating efficiently and effectively.*

This report addresses a top EPA management challenge:

- *Enhancing information technology security.*

Address inquiries to our public affairs office at (202) 566-2391 or OIG_WEBCOMMENTS@epa.gov.

List of OIG reports.

EPA Needs to Improve Processes for Securing Region 8's Local Area Network

What We Found

Exploitation of vulnerabilities may result in the loss of confidentiality, integrity, and availability of personally identifiable information and scientific data.

The vulnerability tests of Region 8's local area network, conducted by the EPA's Office of Mission Support, were not comprehensive. Additionally, wireless networks operating within the Region 8 laboratory could jeopardize controls protecting vulnerable laboratory equipment. If vulnerabilities at Region 8 are exploited, there could be denial-of-service attacks, unauthorized disclosure of personally identifiable information, and corruption of scientific data that are used to make program decisions.

The lack of updated SCORPIOS technical documentation, the Office of the Chief Financial Officer's inability to identify whether personally identifiable information is secured on regional SCORPIOS servers, and the security concerns raised in two 2019 hotline complaints regarding SCORPIOS warrant an OCFO investigation of whether SCORPIOS needs additional controls to protect the confidentiality, integrity, and availability of the system. A future breach to the SCORPIOS application could cost the EPA $11,477,250.

Recommendations and Planned Agency Corrective Actions

We recommend that Region 8 update its local area network system security plan and review wireless access points within the Region 8 laboratory. We further recommend that the Office of Mission Support review and implement procedures to verify that vulnerability tests and their results are comprehensive. We also recommend that the OCFO implement internal controls to protect personally identifiable information and manage system development for the SCORPIOS application.

The Agency concurred with our recommendations and provided acceptable corrective actions. The Agency has completed corrective actions for four of our seven recommendations. We consider the remaining three recommendations resolved with corrective actions pending.

UNITED STATES ENVIRONMENTAL PROTECTION AGENCY
WASHINGTON, D.C. 20460

THE INSPECTOR GENERAL

September 10, 2020

MEMORANDUM

SUBJECT: EPA Needs to Improve Processes for Securing Region 8's Local Area Network
Report No. 20-E-0309

FROM: Sean W. O'Donnell Sean W O'Donnell

TO: Donna Vizian, Principal Deputy Assistant Administrator
Office of Mission Support

Gregory Sopkin, Regional Administrator
Region 8

David Bloom, Deputy Chief Financial Officer

This is our report issued on the subject evaluation conducted by the Office of Inspector General of the U.S. Environmental Protection Agency. The project number for this evaluation was OA&E-FY20-0111. This report contains findings that describe the problems the OIG has identified and corrective actions the OIG recommends. Final determination on matters in this report will be made by EPA managers in accordance with established audit resolution procedures.

The Office of Mission Support has primary responsibility for running vulnerability tests of the Agency's information systems. Region 8 has primary responsibility for evaluating and remediating vulnerabilities identified on its local area network. The Office of the Chief Financial Officer has primary responsibility for issues related to the Superfund Cost Recovery Imaging and Online System.

In accordance with EPA Manual 2570, your office provided acceptable corrective actions and estimated milestone dates in response to OIG recommendations. All recommendations issued in this report are either completed or resolved, and no final response to this report is required. However, if you submit a response, it will be posted on the OIG's website, along with our memorandum commenting on your response. Your response should be provided as an Adobe PDF file that complies with the accessibility requirements of Section 508 of the Rehabilitation Act of 1973, as amended. The final response should not contain data that you do not want to be released to the public; if your response contains such data, you should identity the data for redaction or removal along with corresponding justification.

We will post this report to our website at www.epa.gov/oig.

Table of Contents

Appendices

Purpose

Top Management Challenge

This evaluation addresses the following top management challenge for the Agency, as identified in OIG Report No. 20-N-0231, *EPA's FYs 2020–2021 Top Management Challenges*, issued July 21, 2020:

- Enhancing information technology security.

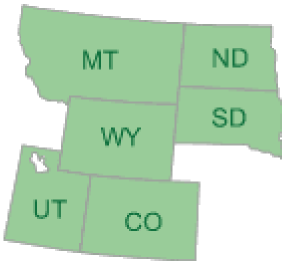
The U.S. Environmental Protection Agency's Office of Inspector General performed this evaluation to (1) assess the completeness of EPA processes for testing its network to identify potential vulnerabilities that could compromise the Agency's systems and data, and (2) conduct independent automated vulnerability testing of information technology resources connected to the EPA's network to identify vulnerabilities that could be used to compromise the confidentiality, integrity, and availability of Agency information systems and data.

Background

Information systems are necessary to carry out the organization's mission and business functions; therefore, it is necessary to protect the confidentiality, integrity, and availability of the data within those systems. The National Institute of Standards and Technology developed a Risk Management Framework to improve information security and strengthen the risk management process for federal information systems. In July 2016, the Office of Management and Budget revised Circular A-130, *Managing Information as a Strategic Resource*, to require federal agencies to be responsible for privacy programs under the Risk Management Framework.

The EPA has ten regional offices that are responsible for the execution of EPA programs within several states and territories (Figure 1). Region 8 serves Colorado, Montana, North Dakota, South Dakota, Utah, Wyoming, and 28 tribal nations. The Region 8 local area network provides resources for the Region's headquarters office, laboratory, and satellite office in Helena, Montana. Region 8's Laboratory Services and Applied Sciences Division play a critical role in protecting human health and the environment by analyzing air, water, soil, and biota samples. The Region 8 laboratory standalone LAN includes laboratory equipment, printers, computers, and network devices. Region 8 representatives indicated that the standalone laboratory network was established to remediate the risk of vulnerabilities.

Figure 1: Map of EPA Region 8



Source: EPA website. (EPA image)

A **local area network** is a group of computers and devices that reside in a limited area and can interact with each other.

When vulnerabilities are found within Region 8, the Region must report, track, and remediate the weakness. The EPA's Chief Information Officer's CIO 2150-P-04.2, *Information Security – Security Assessment and Authorization Procedures*, dated May 27, 2016, requires Agency personnel to document information security weaknesses and planned remedial actions in the Agency's information security tracking system.

Responsible Offices

The Office of Mission Support leads the EPA's information management and information technology programs, which provide the necessary services to support the Agency's mission to protect human health and the environment. Within the OMS, the National Computer Center, or NCC, Security Branch's Network Security Operations Center Vulnerability Management Team is responsible for conducting vulnerability tests of the Agency's information systems. Per CIO 2150-P-14.2, *Information Security – Risk Assessment Procedures*, dated April 11, 2016, the NCC's branch conducts vulnerability tests for all of the EPA's information systems and applications at least every 72 hours.

The Office of the Chief Financial Officer's Office of Technology Solutions is the system owner for the Superfund Cost Recovery Package Imaging and Online System application. SCORPIOS servers are installed at each region and finance center.

The Region 8 Mission Support Division is responsible for managing the operations of Region 8's LAN, which includes remediating vulnerabilities identified by the OMS's vulnerability testing.

Scope and Methodology

We conducted this evaluation from January through June 2020 in accordance with the *Quality Standards for Inspection and Evaluation* published in January 2012 by the Council of the Inspectors General on Integrity and Efficiency. Those standards require that we obtain sufficient, appropriate evidence to provide a reasonable basis for our findings, conclusions, and recommendations based on our review.

We performed our evaluation at EPA headquarters, Region 8, and the EPA's NCC. We reviewed Region 8's LAN system security plan and interviewed Region 8's Mission Support Division personnel to gain an understanding of the Region's network. We interviewed OMS personnel at the NCC regarding the Agency's vulnerability testing process. We obtained and reviewed the Agency's vulnerability tests for Region 8 and compared the OMS's and the OIG's vulnerability test results. We relied on reports generated by a commercially available tool used to complete the vulnerability tests performed by the OMS and the OIG.

We conducted independent vulnerability tests at Region 8's headquarters, Montana office, and laboratory. We visually verified the Region 8 laboratory standalone LAN by viewing lines connected to devices and running commands on devices within and outside the standalone laboratory LAN.

Due to travel restrictions and mandated telework because of the coronavirus pandemic—that is, the SARS-CoV-2 virus and resultant COVID-19 disease—we did not travel to the NCC to conduct additional vulnerability testing and review the OMS's vulnerability testing process. We also did not return to the Region 8 laboratory to identify and further document all the wireless networks. Instead, we collected evidence from the OMS to help us determine why there was a significant number of vulnerabilities identified by our independent testing compared to the vulnerability testing results that Region 8 provided us.

Subsequent to providing the Agency the draft report, we learned that the Region 8 laboratory shares its building with the Office of Enforcement and Compliance Assurance and that it was possible our wireless testing results identified computer equipment under that office's control. We met with an Office of Enforcement and Compliance Assurance representative, who identified that the office only has limited authorized wireless access points within its conference rooms at the Region 8 laboratory and does not have equipment within Region 8 laboratory's standalone LAN.

While planning this evaluation, the OIG received two anonymous hotline complaints regarding the SCORPIOS application. We reviewed the SCORPIOS system security plan—updated in November 2019—and interviewed OCFO personnel to gain an understanding of the SCORPIOS application. We conducted additional analysis of our vulnerability test results to understand the vulnerabilities that existed on the Region 8 SCORPIOS server. We also reviewed the hotline complaints and identified additional information system security concerns that the OCFO should investigate. These concerns are summarized in Appendix A.

SCORPIOS is used to organize cost information and produce reports that summarize the cost of specific Superfund responses, the Brownfield Program, or oil spill sites.

Results of Evaluation

The OMS and Region 8 need to improve collaboration to better identify vulnerabilities that need to be remediated. For instance:

- The EPA's NCC vulnerabilities testing does not encompass the entire Region 8 network.

- Unidentified wireless networks within the Region 8 laboratory could jeopardize the isolation of vulnerable devices on the laboratory's standalone LAN.

- Significant security concerns regarding the SCORPIOS application warrant that the OCFO further investigate whether additional controls are needed to protect the confidentiality and integrity of the SCORPIOS application.

The National Institute of Standards and Technology Special Publication 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, dated April 2013, requires organizations to (1) employ vulnerability testing tools to perform comprehensive testing and report on vulnerabilities and remediate legitimate vulnerabilities, (2) implement wireless access restrictions, and (3) know the security status of its information systems. The EPA's information security procedures require system owners, in coordination with Agency officials, to perform comprehensive vulnerability tests and to continuously monitor for unauthorized wireless connections.

The **Region 8 LAN** is divided into 35 virtual LANs, which isolate related devices that communicate to each other on different physical locations on the network.

The weaknesses that we identified exist because:

- The Region 8 LAN system security plan, last updated in August 2018, was not current with regard to network information needed to perform comprehensive scans.

- There is no verification of what is included in the Region 8 LAN vulnerability tests prior to or after the OMS performs these tests.

- Region 8 was unaware of the wireless networks in its laboratory.

- The OCFO was not aware of the concerns outlined in the hotline complaints.

As a result, remote attackers could exploit these vulnerabilities to compromise the confidentiality, integrity, and availability of Region 8's LAN. If the Region's LAN and the SCORPIOS application are exploited due to unaddressed security and system development weaknesses, personally identifiable information could be disclosed, network resources could not be accessed, and scientific data would be corrupted.

Agency Vulnerability Tests and Results Are Not Comprehensive

The OMS vulnerability tests and results of the Region 8 LAN were not comprehensive. Per National Institute of Standards and Technology Special Publication 800-53, organizations are required to employ vulnerability testing tools to perform comprehensive testing, report on vulnerabilities, and remediate legitimate vulnerabilities. CIO 2150-P-01.2, *Information Security – Access Control Procedure*, dated September 21, 2015, also requires system owners, in coordination with Agency officials, to perform comprehensive vulnerability tests.

The OMS performs vulnerability tests of the Region 8 LAN every 72 hours and provides results of identified vulnerabilities to the Region for remediation. We found that the OMS's vulnerability test results for the Region 8 LAN were not comprehensive since the list of tested internet protocol addresses excluded one of the Region's 35 virtual LANs.

An **internet protocol address** is an identifier used to communicate with a virtual or physical device connected to the network.

Region 8 relies upon the OMS vulnerability test results without verifying the vulnerability testing configuration. Region 8 personnel indicated that they receive OMS vulnerability testing results but not the configuration of the vulnerability testing software to know which internet protocol addresses were tested. Further, Region 8's LAN system security plan contains outdated internet protocol addresses that are needed to configure the vulnerability testing software to perform comprehensive vulnerability testing. If the NCC relied upon the Region 8 LAN system security plan for identifying internet protocol addresses, the vulnerability test would be incomplete because the information is inaccurate.

After we provided the draft report to the Agency, the OMS made us aware that, during our evaluation, it was phasing in an updated vulnerability testing process. During our fieldwork, Region 8 provided us with vulnerability testing results for the Region. These results did not cover the entire Region 8 network since the OMS only provided Region 8 with vulnerabilities identified on one of the 35 Region 8 virtual LANs. We later discovered that at the time of our evaluation, the OMS was only providing Region 8 with vulnerability testing results for select Region 8 servers. This led to a discrepancy between the number of vulnerabilities we identified from our independent testing and the number of vulnerabilities Region 8 knew existed on its network. In May 2020, the OMS provided Region 8 with more comprehensive vulnerability testing results.

Unidentified Wireless Access Points at Region 8 Laboratory

Unidentified wireless access points could compromise the security of vulnerable Region 8 laboratory equipment. The National Institute of Standards and Technology Special Publication 800-53 requires organizations to implement restrictions to wireless access. CIO 2150-P-01.2 requires system owners, in coordination with Agency officials, to implement and enforce requirements for using wireless connections to EPA systems and to continuously monitor for unauthorized wireless connections.

While testing the Region 8 laboratory, we identified several wireless access points within the boundaries of the Region 8 laboratory. When we brought this issue to a Region 8 representative, the representative was unaware of devices within the Region 8 laboratory with wireless configurations enabled. Region 8 personnel also could not identify whether the wireless access points we identified were attributed to the Region 8 laboratory or the Office of Enforcement and Compliance Assurance's National Enforcement Investigation Center. However, Region 8 personnel indicated that it is possible laboratory equipment connected to the laboratory network may have had wireless capabilities enabled by default.

OCFO Needs to Address the Security of SCORPIOS

The SCORPIOS application contains security concerns that jeopardize the confidentiality, integrity, and availability of the system. We also noted that the SCORPIOS application configuration documentation is outdated. For example, the documentation on the SCORPIOS website indicates that SCORPIOS must run on a software platform that the vender ended all support for on December 31, 2002. Additionally, during our discussions with OCFO representatives, they indicated that they are unable to readily identify all records containing PII and have difficulty accessing PII on regional SCORPIOS databases.

During the planning of this evaluation, the OIG Hotline received two complaints (Appendix A) alleging that:

- The OCFO and the OMS stored extracts of sensitive PII from SCORPIOS on the EPA network without adequate protection from unauthorized disclosure.

- The OCFO failed to provide adequate oversight while implementing a system to replace SCORPIOS.

We summarized the main concerns of the complaints to make the OCFO aware that these allegations, coupled with the OIG's findings above, noted vulnerabilities on the Region 8 SCORPIOS server that warrant investigation. Most notably, OIG Report No. 20-F-0033, *EPA's Fiscal Years 2019 and 2018 (Restated) Consolidated Financial Statements*, dated November 19, 2019, reported a similar finding regarding the protection of PII on OCFO servers hosted at the EPA's NCC. In that report, we stated that sensitive PII was stored in plain text files and access was not adequately restricted. The OCFO indicated that it completed the agreed-to corrective actions for the related recommendations at the end of calendar year 2019. We will follow up on these corrective actions during the 2020 financial statement audit.

We estimate that a future SCORPIOS breach could cost the EPA $11,477,250. This estimate is based on SCORPIOS containing 76,515 records that include sensitive PII and the average cost of a data breach, which is $150 per record. The record count is based on tables containing PII that could be readily identifiable. OCFO representatives indicated that SCORPIOS contains other PII that could not be readily identified.

Conclusions

By not providing comprehensive tests and results, the EPA may be unaware of vulnerabilities that could cause denial-of-service attacks, unauthorized disclosure of PII and sensitive PII, and corruption of the integrity of Region 8 laboratory's scientific data. A future breach to EPA information systems that contain PII may cost the EPA $11,477,250.

Recommendations

We recommend that the Region 8 regional administrator:

1. Update the Region 8 network information in the Region's local area network system security plan.

2. Review the configurations of Region 8 laboratory equipment and disable wireless capabilities on equipment not authorized to connect to wireless networks.

We recommend that the assistant administrator for Mission Support:

3. Develop and implement procedures to verify that the internet protocol addresses being tested contain all the location's networked equipment.

4. Identify deficiencies preventing the Office of Mission Support vulnerability tests from producing complete results, and create plans of action and milestones to correct identified deficiencies in the Agency's vulnerability testing and reporting process.

We recommend that the chief financial officer:

5. Update the Superfund Cost Recovery Package Imaging and Online System configuration document to identify the current operating system platforms required to operate the application.

6. Coordinate with regions to implement internal controls to determine whether personally identifiable information is protected on regional Superfund Cost Recovery Package Imaging and Online System servers.

7. Provide the OIG with a written response on the actions taken or planned to address the hotline complaint allegations related to the Superfund Cost Recovery Package Imaging and Online System within 30 days of this report.

Agency Response and OIG Assessment

Subsequent to providing the Agency the draft report, we removed two recommendations regarding vulnerability scan results after the OMS and Region 8 provided additional information.

The Agency concurred with all the remaining recommendations and provided acceptable planned corrective actions and estimated completion dates:

- Region 8 agreed with Recommendations 1 and 2 and provided documentation of completed corrective actions. We consider these recommendations completed.

- The OMS agreed with Recommendations 3 and 4 and provided acceptable planned corrective actions and estimated completion dates. We consider these recommendations resolved with corrective actions pending.

- The OCFO agreed with Recommendations 5, 6, and 7. The OCFO provided documentation of completed corrective actions for Recommendations 5 and 7. We consider these recommendations completed. The OCFO provided an acceptable planned corrective action and estimated completion date for Recommendation 6. We consider this recommendation resolved with corrective actions pending.

The Agency's responses to our draft report are in Appendix B. The Agency also provided additional documentation for our consideration, and we revised the report as appropriate.

Status of Recommendations and Potential Monetary Benefits

RECOMMENDATIONS

Rec. No.	Page No.	Subject	Status[1]	Action Official	Planned Completion Date	Potential Monetary Benefits (in $000s)
1	7	Update the Region 8 network information in the Region's local area network system security plan.	C	Region 8 Regional Administrator	8/12/20	
2	7	Review the configurations of Region 8 laboratory equipment and disable wireless capabilities on equipment not authorized to connect to wireless networks.	C	Region 8 Regional Administrator	8/21/20	
3	7	Develop and implement procedures to verify that the internet protocol addresses being tested contain all the location's networked equipment.	R	Assistant Administrator for Mission Support	4/15/21	
4	7	Identify deficiencies preventing the Office of Mission Support vulnerability tests from producing complete results, and create plans of action and milestones to correct identified deficiencies in the Agency's vulnerability testing and reporting process.	R	Assistant Administrator for Mission Support	10/31/21	
5	7	Update the Superfund Cost Recovery Package Imaging and Online System configuration document to identify the current operating system platforms required to operate the application.	C	Chief Financial Officer	8/31/20	
6	7	Coordinate with regions to implement internal controls to determine whether personally identifiable information is protected on regional Superfund Cost Recovery Package Imaging and Online System servers.	R	Chief Financial Officer	10/30/20	$11,477,000
7	8	Provide the OIG with a written response on the actions taken or planned to address the hotline complaint allegations related to the Superfund Cost Recovery Package Imaging and Online System within 30 days of this report.	C	Chief Financial Officer	8/7/20	

[1] C = Corrective action completed.
R = Recommendation resolved with corrective action pending.
U = Recommendation unresolved with resolution efforts in progress.

Appendix A

Summary of SCORPIOS Hotline Complaints

The OIG Hotline received the first SCORPIOS complaint in November 2019, which contained the following allegations:

- The acting chief financial officer and CIO collaborated to copy sensitive PII (dating back to 1996) and confidential business information located in unencrypted files on the NCC network, forgoing establishing security controls, resulting in a SCORPIOS breach in 2015 costing the EPA over $200,000.

- The acting chief financial officer and CIO planned to make these files available to headquarters and regional offices for "reporting and system interface purposes," without masking PII or restricting access on a need-to-know basis.

The OIG Hotline received a second complaint in December 2019, which contained the following allegations:

- During the "2019 FINTECH conference," "Executive Leadership" made misleading and deceptive statements that the SCORPIOS replacement, called the E-Recovery system, would be implemented in 2019, despite knowing that the project was less than 50 percent complete and that the 2019 completion date was unattainable. The test of the partial application code received from the vendor resulted in multiple errors. At that time, the e-Recovery system was estimated to cost $1.5 million.

- Due to the government shutdown at the end of 2018 and beginning of 2019, the time-and-materials contract to develop the E-Recovery system received a six-month extension; however, the contract expired "without receipt of the final application program code or any system of lifecycle documentation," preventing the OCFO from implementing the E-Recovery system.

- Once the e-Recovery system program manager became aware that requirements were not being tracked, the project manager led an analysis that determined 400 requirements were not being met.

- The E-Recovery system project requirements do not define and properly identify the security requirements necessary to correct SCORPIOS's deficiencies.

- Increased costs related to delays and the need to implement additional security controls are not being communicated to the "superfund community that will be utilizing the system, the CIO's Office, and adjustments to the CPIC or FITARA documentation have not been updated."

Appendix B

Agency Responses to Draft Report

We received two responses from the Agency. Each response is copied below in order of recommendation applicability.

UNITED STATES ENVIRONMENTAL PROTECTION AGENCY
WASHINGTON, D.C. 20460

MEMORANDUM

SUBJECT: Response to Office of Inspector General Draft Report Project No. OA&E-FY20-0111, *EPA Needs to Improve Processes for Securing Region 8's Local Area Network*

FROM: Vaughn Noga, Chief Information Officer
Deputy Assistant Administrator for Environmental Information

VAUGHN NOGA
Digitally signed by VAUGHN NOGA
Date: 2020.08.18 15:59:10 -04'00'

Rick Buhl,
Region 8 Mission Support Director

RICHARD BUHL
Digitally signed by RICHARD BUHL
Date: 2020.08.19 08:26:37 -06'00'

TO: Rudy Brevard
Director, Information Resources Management Directorate
Office of Audit and Evaluation

Thank you for the opportunity to respond to the issues and recommendations in the subject audit report, "*EPA Needs to Improve Processes for Securing Region 8's Local Area Network*," dated August 7, 2020. The Office of Mission Support is providing responses to recommendations 3 and 4 and region 8 is providing responses to recommendations 1 and 2.

AGENCY'S OVERALL POSITION

The agency concurs with the recommendations of this report and has included a summary response with high-level corrective actions and target completion dates in the table below.

OMS RESPONSE TO REPORT RECOMMENDATIONS

No.	Recommendation	Action Official	High-Level Intended Corrective Action(s)	Estimated Completion Date
1	Update the region 8 network information in the region’s local area network system security plan.	Region 8	Review and Update the region 8 System Boundaries in the System Security Plan. a. Review the all asset scans of the region 8 Denver, Colorado, HQ building and the Helena, Montana, Field Office and determine which assets are: 1. The responsibility of region 8 and directly supported by regional staff. 2. The responsibility of region 8 and supported by contractors to region 8. 3. Located in region 8 but the responsibility of other support. E.G. the LANES national contract, OITO assets such as the BigFix or SCCM systems, and etc… b. Repeat this process using the OISPprovided “All Asset” scans which run every 72 hours. c. Request the current system boundary reported to OISP and update this. Update the system boundary in the region 8 System Security Plan in Xacta.	Completed August 12, 2020

2	Review the configurations of region 8 laboratory equipment and disable wireless capabilities on equipment not authorized to connect to wireless networks.	Region 8	Address the OIG finding by confirming the configuration of equipment connected to the region 8 air-gapped lab network and conduct a wireless survey to identify the wireless access points accessible to equipment in the region 8 lab. a. Region 8 systems administration staff review the configuration settings of equipment on the region 8 air-gapped network. Completed August 12, 2020. b. Region 8 Information Security Officer conduct wireless survey at the region 8 Lab. Scheduled for completion August 21, 2020. 1. Using a standard laptop identify all wireless access points accessible to equipment in the lab. 2. Review the list to identify the parties responsible for each identified point. Report the list to OISP and determine if any of the identified points require further action by region 8 and/or OISP. Create POA&Ms as needed.	August 21, 2020
3	Develop and implement procedures to verify that the internet protocol addresses being tested contain all the location's networked equipment and locations.	OMS	Develop and implement a process to verify IP addresses on the agency's network addressable systems. a. Review and update lists of identified IP addresses and network segments with PO/R POCs. b. Update enterprise monitoring tools as needed. c. Verify IP addresses periodically with enterprise monitoring tools.	April 15, 2021

4	Identify deficiencies preventing the OMS vulnerability tests from producing complete results and create plans of action and milestones to correct identified deficiencies in the agency’s vulnerability testing and reporting process.	OMS	Develop and implement a process to analyze corrective measures. a. Review and update deficiencies with PO/R POCs. b. Update enterprise monitoring tools as needed.	October 31, 2021

If you have any questions regarding this response, please contact Mitch Hauser, audit follow-up coordinator, of the Office of Mission of Support, (202) 564–7636.

Cc: Nii-Lantei Lamptey
Christina Nelson
Teresa Richardson
Albert Schmidt
Jeff
Anouilh
Lee
Kelly
Dan Coogan
Jan Jablonski
Monisha Harris
Marilyn Armstrong
Mitchell Hauser
Allison Thompson
Matt Duran
Nikki Wood
Andrew LeBlanc

UNITED STATES ENVIRONMENTAL PROTECTION AGENCY

WASHINGTON, D.C. 20460

August 10, 2020

OFFICE OF THE
CHIEF FINANCIAL OFFICER

MEMORANDUM

SUBJECT: Response to the Office of Inspector General Draft Audit Report, Project No. OA&E-FY20-0111, *"EPA Needs to Improve Processes for Securing Region 8's Local Area Network,"* July 10, 2020

FROM: *(for)* David A. Bloom, Deputy Chief Financial Officer
Office of the Chief Financial Officer

CAROL TERRIS

Digitally signed by CAROL TERRIS
Date: 2020.08.10
17:09:38 -04'00'

TO: Rudolph M. Brevard, Director
Information Resources Management Directorate Office of Audit and Evaluation

Thank you for the opportunity to respond to the issues and recommendations in the subject draft audit report. The following is a summary of the OCFO's overall position on the report recommendations.

OVERALL POSITION

The OCFO concurs with the Office of Inspector General's recommendations. Details on the audit recommendations are provided in the table, below. The italics section is the complaint, and the second is the response.

RESPONSE TO RECOMMENDATION #9

This recommendation requests a response to the December 2019 Hotline request. The OIG Hotline received the first SCORPIOS complaint in November 2019, and it contained the following allegations:

Hotline complaint: The acting Chief Financial Officer and CIO collaborated to copy sensitive PII (dating back to1996) and confidential business information located in unencrypted files on the NCC network, forgoing establishing security controls, resulting in a SCORPIOS breach in 2015, costing the EPA over $200,000.

Response: In 2015, Scorpios had a data breach that was caused by a contractor neglecting to follow the security guidelines in place during that time. After a thorough review EPA deemed it necessary to offer credit monitoring to the impacted community. Since that time, the corrective actions have all been implemented.

Hotline complaint: The acting Chief Financial Officer and CIO plan to make these files available to headquarters and regional offices for "reporting and system interface purposes," without masking PII or restricting access on a need-to-know basis.

Response: OCFO only makes data available in Scorpios to headquarters and regional staff on a need-to know basis as approved through the system access request form.

Please find our response to the five areas identified in the hotline request from December 2019.

Hotline complaint: During the "2019 FINTECH conference," "Executive Leadership" made misleading and deceptive statements that the SCORPIOS replacement, called the E-Recovery System, would be implemented in 2019, despite knowing that the project was less than 50 percent complete and that the 2019 completion date was unattainable. The test of the partial application code received from the vendor resulted in multiple errors. At that time, it was estimated to cost $1.5 million.

Response: The complaint is not accurate. At the 2019 FINTECH, a demo of the completed work at the time was conducted, and it was well received by the Superfund Community. The reference to the project being less than 50% complete is not based on the actual work completed. The project effort used incremental development techniques which meant that after each function was completed, testing was conducted to ensure it functioned as expected and was on target to complete as planned. It is normal in incremental development and testing that projects defects are routinely identified and logged for correction. This data and subsequent resolution for issues that were identified is documented in the Sprint Release notes for each sprint. All costs have been accurately reflected against the IT code established for E-Recovery, reported through the agency's accounting and the CPIC system. It is not clear what the $1.5 M mentioned in the complaint is in reference to.

Hotline complaint: Due to the government shutdown in the end of 2018 and the beginning of 2019, the time and materials contract to develop the E-Recover System received a six-month extension; however, the contract expired "without receipt of the final application program code or any system of lifecycle documentation," preventing the OCFO from implementing the E-Recovery project.

Response: The contract did expire, but EPA does have the code developed to this point, and all project documentation is properly maintained in our Project Web Application. Unexpected budget cuts in FY 2020 led to some difficult decisions on priorities, and that has meant additional delays for this project. The completion of the project requires the final sprints to be completed, which include the security functions. Because security touches all modules for the system, it was required to be the last development sprint, and accompanying documentation, to be completed.

Hotline complaint: Once the program manager became aware that requirements were not being tracked, the project manager led an analysis that determined 400 requirements were not being met.

Response: The Program Manager conducted a review of the project to ensure an efficient restart once the new contract was in place. It was identified during the Program Review that 136 requirements were not detailed enough for proper development and required additional clarification before the work under the replacement contract can be started. A full Requirements Traceability Matrix (RTM) is on file, and the three rounds of requirements documents developed in conjunction with the Superfund Community and the signatures are on file as well. The RTM contains 852 Requirements.

Hotline complaint: The E-Recovery's project requirements does not define and properly identify the security requirements necessary to correct SCORPIOS's deficiencies.

Response: The security requirements were identified for this effort. The first place these are evident is in the design and architecture, which are the primary area where SCORPIOS Security Deficiencies were being addressed. There are additional details documented in the EPA SCORPIOS Security Feature - Architecture Comments because the security module was the last module to be completed the Security team has taken the opportunity presented by the Program Review to identify additional security requirements not previously identified which the team will incorporate into the final product where they are applicable.

Hotline complaint: Increased costs related to delays and the need to implement additional security controls are not being communicated to the "superfund community that will be utilizing the system, the CIO's Office, and adjustments to the CPIC or FITARA documentation have not been updated.

Response: The Superfund Community is a part of our SCORPIOS Stakeholder Group, which meet monthly, and are given regular updates on the status of this project. Because the new contract has not yet been awarded, the team can only provide high level contract updates at this time. The costs associated with every IT Project have an IT code which populates accounting system reports and the CPIC data automatically, which means the costs are accurately reflected and are visible to all within the agency. FITARA approvals for the new contract to support the final sprints were conducted, approved, and are on file. Additionally, as part of the Annual IT Portfolio Review, all OCFO IT Project costs and efforts are discussed.

RESPONSE TO DRAFT AUDIT RECOMMENDATIONS

Agreements

No.	Recommendation	Assigned to:	High-Level Corrective Action(s)	Estimated Completion Date

7	Update the Superfund Cost Recovery Package Imaging and Online System configuration document to identify the current operating system platforms required to operate the application.	OCFO	Concur. Attached is the SCORPIOS System Administrator document version 4.0 dated February 2011. The document includes the system configuration section (section #2). The document is being updated and will be finalized and finished, with a target date of August 31, 2020.	8/31/20
8	Coordinate with regions to implement internal controls to determine whether personally identifiable information is protected on regional Superfund Cost Recovery Package Imaging and Online System servers.	OCFO	Concur. OCFO/OTS will coordinate with EPA Regions to implement a Memorandum of Understanding. The intent is for the MOU to require each Regional Senior Information Official to certify that PII on regional SCORPIOS servers is protected in accordance with EPA's IT Security policies. Estimated timing to complete the documents is October 30, 2020. In addition to the MOU with each of the EPA Regions, the OCFO has identified nearly 20,000 PII records that may be appropriate for removal from the regional databases. The OCFO will work with regional contacts to verify and delete the records which will further reduce risk of PII disclosure.	10/30/20
9	Provide the OIG a written response on the actions taken or planned to address the hotline complaint allegations related to the Superfund Cost Recovery Package Imaging and Online System within 30 days of this report.	OCFO	Concur. A response to each allegation has been provided in the body of this memorandum.	Completed 8/7/20

CONTACT INFORMATION

If you have any questions regarding this response, please contact the OCFO Audit Follow-up Coordinator, Andrew LeBlanc, at leblanc.andrew@epa.gov or (202) 564-1761.

cc: Carol Terris
C. Paige Hanson
Lek Kadeli
Charlie Dankert
Jeanne Conklin
Meshell Jones-Peeler
Eva Ripollone
Istanbul Yusuf
Richard Gray
OCFO-OC-MANAGERS
Albert Schmidt
Teresa Richardson
Andrew LeBlanc
José Kercadó-Deleon

Appendix C

Distribution

The Administrator
Assistant Deputy Administrator
Associate Deputy Administrator
Chief of Staff
Deputy Chief of Staff/Operations
Chief Financial Officer
Agency Follow-Up Coordinator
General Counsel
Assistant Administrator for Mission Support
Regional Administrator, Region 8
Associate Administrator for Congressional and Intergovernmental Relations
Associate Administrator for Public Affairs
Director, Office of Continuous Improvement, Office of the Administrator
Deputy Chief Financial Officer
Associate Chief Financial Officer
Associate Chief Financial Officer for Policy
Controller
Deputy Controller
Principal Deputy Assistant Administrator for Mission Support
Associate Deputy Assistant Administrator for Mission Support
Deputy Regional Administrator, Region 8
Deputy Assistant Administrator for Environment Information and Chief Information Officer, Office of Mission Support
Senior Information Officer, Office of Mission Support
Director, Policy, Training and Accountability Divison, Office of the Controller
Director, Office of Resources and Business Operations, Office of Mission Support
Director, Administrative IT Staff, Office of Mission Support
Director, Information Security and Management Staff, Office of Mission Support
Director, Office of Regional Operations
Branch Chief, Management, Integrity and Accountability Branch, Policy, Training, and Accountability Division, Office of the Controller
Audit Follow-Up Coordinator, Office of the Administrator
Audit Follow-Up Coordinator, Office of the Chief Financial Officer
Audit Follow-Up Coordinator, Office of Mission Support
Audit Follow-Up Coordinator, Region 8